

3215
April 30, 1968APOLLO APPLICATIONS
PROGRAM DIRECTIVE NO. 13

TO : Distribution FROM:


DIRECTOR, APOLLO APPLICATIONSSUBJECT : AAP Failure Mode and Effect Analysis; Single
Failure Point Identification and ControlREFERENCES : (a) Apollo Applications Reliability and Quality
Assurance Program Plan, NHB 5300.5, May 1967
EditionI. PURPOSE

The purpose of this directive is to elaborate on the basic FMEA/SFP requirements established in Reference (a). These requirements are summarized as follows: (1) Accomplishment of FMEA's for all AAP Flight and Flight Support Equipment, (2) Identification and analysis of SFP's, (3) Reporting of category 1, 2, A and B SFP's (and rationale for retention) at major program milestones, (4) Establishment of a management control system to minimize the impact of these SFP's on Crew Safety and the accomplishment of mission objectives, (5) Establishment of contingency/emergency procedures for Category 1, 2, A and B SFP's and (6) Furnishing of FMEA/SFP results to appropriate Test personnel as a primary consideration in test planning, monitoring, and overall test emphasis.

The specific objectives of this directive are:

- A. To establish a baseline procedure for accomplishing and reporting FMEA's and SFP analysis.
- B. To establish FMEA/SFP requirements for various operational modes and hardware levels.

- C. To establish requirements for submission of FMEA results to Mission Operations as basic inputs to the Mission Planning Activities (i.e., preparation of contingency procedures/mission rules, failure symptom analyses, training requirements, Crew Operations Handbook, etc.)
- D. To establish FMEA/SFP requirements relative to significant design changes.
- E. To establish requirements for updating and evaluation of FMEA/SFP results for each specific mission.
- F. To establish minimum requirements and procedures for a Management Control System for SFP's.

II. SCOPE

This directive is applicable to all NASA activities with cognizance over design and development of AAP flight equipment, launch complex equipments, and related support equipments which have major impact on the accomplishment of mission objectives. This includes the AAP Program Office, the Center Program Offices, and their Resident Offices at contractor facilities.

III. POLICY AND REQUIREMENTS

- A. The AAP Reliability and Quality Assurance Program Plan, NHB 5300.5, establishes the requirements for development of failure mode and effect analyses and for assuring the reporting and controlling of single failure points.
- B. One of the primary objectives of the AAP Reliability Program is to identify all significant single failure point potentials for each equipment for various modes of operation. For each mission, these single failure point potentials will be examined to determine which potentials are truly single failure points and a summary of these single failure points will be prepared and kept current. Program Directors will review/buy-off these SFP's at major program milestone reviews (see Figure 1).

- C. Supporting information from Apollo failure mode and effect analyses delineating equipment failure modes, failure effects or failure consequences will be utilized to the maximum extent possible.
- D. Baseline Procedures. Failure mode and effect analyses must be extended beyond effects on equipment operation to include the related effects on attainment of mission objectives, including safety of the crew. Two types of analyses are used to satisfy this requirement - Mission Level FMEA's and Equipment Level FMEA's.
1. Mission Level FMEA. The first type of analysis is the Mission Level FMEA whose objective is to delineate from the "top down" those critical functions and related hardware which can lead to specific consequences to given mission objectives or to crew/personnel safety. The results of this analysis bridge the gap between equipment and mission by singling out only the critical hardware items which are truly single failure points for the mission being examined. It is recognized that differences in mission complexity and hardware complexity dictate the use of special analyses. To this end, mission level FMEA's shall be performed utilizing an approach that (1) clearly translates hardware and supporting functional effects to effect on mission objectives, and (2) provides information suitable for developing single failure point summaries at the mission level. A separate mission level FMEA shall be developed for the pre-launch phase of the mission which will consider all launch support equipment including interfaces with space vehicle. Mission level FMEA shall be accomplished as prescribed in Section IV of this directive.
 2. Equipment Level FMEA/SFP. The objective of an equipment FMEA is to identify equipment failure modes and ultimately the consequences of failure in these modes on the performance of subsystems which are comprised of these equipments. These requirements can be satisfied by following a procedure similar to that contained Attachment A. It is recognized that equipment complexity and use dictates the level of detail to which an equipment FMEA is implemented such that it is not

always mandatory to examine the equipment at the piece part or component level. The significant results of these equipment FMEA's are reported as single failure point potentials for the equipment, and will be used as building blocks to support Mission Level FMEA's.

E. Phasing and Milestones. Figure 1 illustrates the FMEA/SFP requirements in terms of the hardware level at which the effects of failure need to be determined for each major program milestone.

1. Preliminary Design Reviews of AAP flight and ground support equipment require an initial assessment of failure modes and single failure point potentials at both the detailed hardware and stage/module levels and an initial look at the mission FMEA.
2. Critical Design Reviews of this equipment require a more definitive look at these failure modes, single failure point potentials and their consequences. This information is provided through updates of the preliminary FMEA's at all levels.
3. Factory acceptance via Configuration Inspection and Certification of Flight Worthiness requires a further update of the FMEA at the mission and stage/module level and a final look at the detailed hardware level FMEA's.
4. For manned missions an update of the mission FMEA will be required at the Design Certification Review with a final look at the Flight Readiness Review. For unmanned missions this update of the mission FMEA will not be required until the Flight Readiness Review.

F. Application of FMEA and SFP Summaries to Design and Development. The use of previously developed hardware by the Apollo Applications Program will reduce the degree to which FMEA and SFP Summaries are utilized in the basic design activity. However, FMEA/SFP's developed in conjunction with previously developed hardware should be

April 30, 1968

fully reviewed relative to utilization of such hardware and updated where necessary. For those AAP peculiar hardware elements and the significant modification efforts for Apollo hardware, FMEA and SFP Summaries will be used as a primary tool in design evaluation. Specifically, the failure mode analysis portion of the FMEA will be utilized to achieve the AAP Reliability Program goal of identifying the significant failure modes of each hardware equipment and minimizing the impact of these failure modes on the accomplishment of mission objectives. In addition, the FMEA provides a significant input to the definition of display and control requirements. Significant Engineering Change Proposals (ECP's) will be accompanied by appropriate modifications to the existing FMEA's to insure that no unforeseen failure modes are interjected into the system.

G. Application of FMEA and Single Failure Point Summaries to Test Operations. Failure mode and effect analysis and single failure point summaries are to be utilized as an important criterion for AAP hardware test planning.

1. Single Failure Point Summaries shall be submitted to Test Operations as an input for the establishment of checkout procedures. They should be used to select items to be tested, establish modes of operation which must be included, determine frequency of monitoring and determine overall test emphasis. System test data shall be used to update the failure mode effect analysis and SFP Summary.
2. The FMEA shall be submitted to Test Operations as an input to fault isolation and as an input to identifying safety hazards associated with the test.

H. Application of FMEA and SFP to Mission Operations. The primary application of the FMEA and SFP listing to the operations phase of a program is accomplished by providing support to the preparation of mission rules. The single failure points which have been identified provide the definition of contingencies which must be accounted for in the development of alternate modes of operation

and abort planning (pre-launch and in-flight operations). The failure mode and effect analysis provides a significant input to the definition of fault isolation procedures.

This analysis also supports the iterative process of mission planning in the following ways:

1. If special considerations dictate that abort or alternate mode of operation be initiated when a portion of a redundant unit fails, the item under consideration should be added to the single failure point summary as a special entry so that special attention and control will be applied.
2. When alternate modes of operation or aborts have been defined, some will be significant in terms of loss of redundancy, extended time of accomplishment, complexity, marginal performance. Special FMEA's should be accomplished (on a selective basis) to identify the single failure points on the abort or alternate mission. This will provide analysis coverage of special abort and safety systems which were designed as back up systems and received no significant attention during the basic FMEA and SFP activity.
3. FMEA/SFP analyses will be furnished to Mission Operations as an initial listing of significant failure modes, each of which should be explicitly treated in the Mission Rules. Subsequent iterations/updatings of FMEA's will be provided to Mission Operations for incorporation in subsequent iterations of Mission Rules.
4. The Failure Mode and Effect Analysis provides a significant input to both prelaunch and in-flight diagnostic procedures. The identification of equipment which has the potential for, or which already has been evaluated as Single Failure Points, also aids in defining contingencies which must be accounted for in the development of alternate modes of operation (both ground and in-flight), abort planning and astronaut training requirements.

- I. Management Control System for Single Failure Points
Center AAP Configuration Control Boards (CCB)/program managers shall maintain a baseline listing of SFP's (to be provided by appropriate design groups) for each stage/module (by subsystem) beginning at the time of Preliminary Design Review. This listing shall be updated as FMEA's are updated (see figure 1) and as design changes occur. Configuration Control Boards are responsible for insuring that Engineering Change Proposals (ECP) are evaluated for impact on this listing prior to approval of the ECP. All SFP's shall be carefully analyzed for possible elimination and where elimination is not possible/practical, a "rationale for retention (with or without detection)" will be developed. SFP summary listings, using a format similar to that shown in attachment A, figure 3, will be submitted for approval at major program milestone reviews.

IV. RESPONSIBILITIES

- A. NASA Center AAP Program Manager responsibilities for compliance with the requirements of this directive include:
1. Providing resources and personnel at the Center and contractors' facilities for the performance of equipment level FMEA/SFP analyses as defined in this directive. This includes responsibility for insuring that GFE items are considered (as appropriate) in the analyses.
 2. Monitoring the progress of the analyses and measuring results against the stated requirements.
 3. Utilizing the results in support of Program Milestones and in the initiation of action to minimize the effects of Single Failure Point Potentials.
 4. Submitting to the AAP Program Director for approval the rationale for retaining categories 1, 2, A, and B Single Failure Points when corrective action is not implemented.

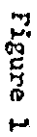
B. An Inter-Center Task Force shall be established for mission level FMEA/SFP analysis. Prime responsibility of this group is to assure the accomplishment of the necessary analyses in support of the major program milestones (see figure 1). Center AAP offices will support the mission level FMEA/SFP activities by providing the following:

1. A representative to act as co-chairman for the above Task Force.
2. Make provisions to have an appropriate contractor representative from each major contractor support this activity as required.
3. Provide sufficient support personnel to work at direction of co-chairman to accomplish task force objectives.

V. DEFINITIONS

Reference (a) shall be used for definition of terms and categories as required in conjunction with the requirements of this directive.

Preliminary	Critical	Configuration Inspection/	Design	Flight
Design Review	Design Review	Certification of	Certification --	Readiness
		Flight Worthiness	Review	Review



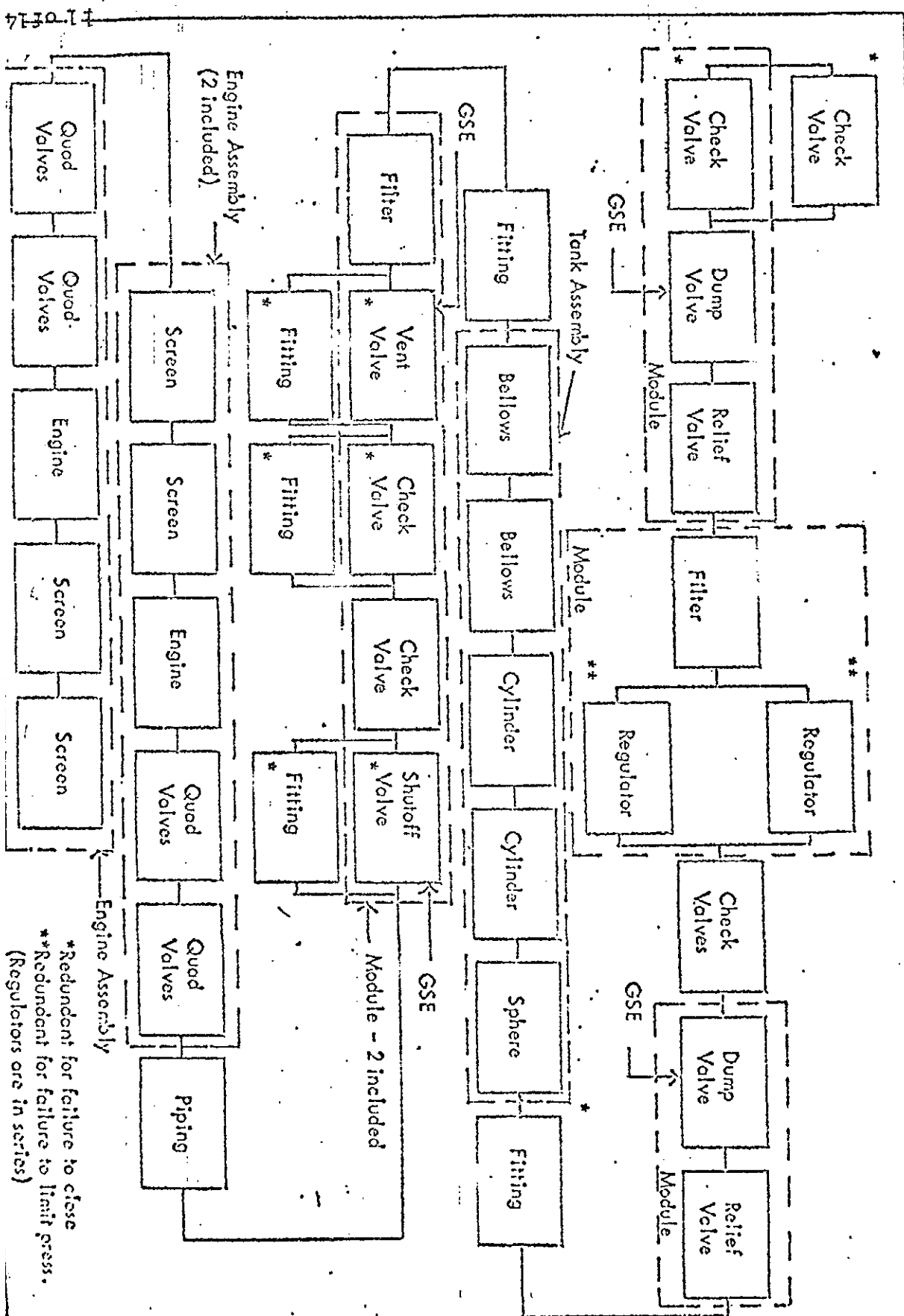
ATTACHMENT A

EQUIPMENT FAILURE MODE & EFFECTS ANALYSES (FMEA) &
SINGLE POINT FAILURE SUMMARY PROCEDURESS

This attachment presents the typical requirements that should be satisfied by equipment Failure Mode & Effect Analyses. An output following this procedure should contain:

- a) Logic Block Diagram, of System under consideration. An example of this is shown in Figure (1) which depicts an Auxiliary Propulsion System of the S-IVB stage as an example.
- b) Failure Mode & Effects Analyses, summary sheet as shown in Figure (2). The description of the requirements as listed in Figure (2) are explained under the appropriate headings of Figure (2).
- c) Single Failure Point Summary sheet as shown in Figure (3), to be completed to the component level or level necessary to describe the single failure point.

AUXILIARY PROPULSION SYSTEM - SIV3 LOGIC DIAGRAM



FAILURE MODE AND EFFECT ANALYSIS

SYSTEM _____

SUBSYSTEM _____

Component	Mission Phase	Failure Mode	Failure Effect
(1) Name of the component under analysis. Break-down of a system for analysis shall be to the component level. Drawing number by which the contractor identifies and describes each component or module. Reference designation used by manufacturer to identify the component or module on the schematic.	(2) Identifies the mission phase(s) for which a component failure made is being considered. (i.e., boost, orbit, final orbit, retrograde and re-entry, landing and post landing).	(3) Give the specific failure mode considering the four basic failure conditions: Premature Operation Failure to operate at a prescribed time. Failure to cease operation at a prescribed time. Failure during operation. Typically, the failure modes are: no output, fail open, fail closed, rupture, etc.	(4) a) Systems b) Other Systems c) Mission/Crew Safety A. Describe the effect of the component failure mode on the system (re-entry control, environmental control, communications, etc). B. Describe the effect of the component failure mode on interfacing systems. C. Describe the effect of the component failure mode on the mission. Add the criticality relating the impact on the system.

Failure Detection		Failure Reaction Time	Recommendations
Flight Crew a) Indication b) Action *	Ground Crew a) Indication b) Action *	(7)	(8)
<p>A. Identify those cues which a particular failure mode presents to the crew (instrument readings, lights, sounds, odors, etc.) Identify instrumentation points by number. Estimate time from failure occurrence to failure indication. B. Describe possible crew action when a failure indication is received. C. Define consequences of undetected failure, if different from Column 4.</p>	<p>A. Identify those cues which a particular failure mode presents to ground monitoring, i.e., the measurements. Estimate time from failure occurrence to failure indication. B. Describe possible ground action, including communications with the crew, when a failure indication is received. C. Define consequences of undetected failure, if different from column 4.</p>		<p>List recommendations with respect to each failure mode (e.g., design changes, inspection techniques, maintenance provisions, checkout capabilities, operations procedures, quality control methods, etc.). Specific methods of how the failure mode can be eliminated must be the primary recommendation when a single component failure can adversely affect the crew or cause the failure of the mission.</p>

* Mission-Level FMEA's only.

* Mission-Level FMEA's only.

Figure 2 (Cont'd.)

SINGLE FAILURE POINT

SINGLE FAILURE POINT SUMMARY

EQUIPMENT

FAILURE CONSEQUENCE

RATIONALE FOR RESENTION
OR CORRECTIVE ACTION

Figure 3

April 30, 1968

DATE

M-D T 3200.089 (Project)

OFFICE OF MANAGED SPACE FLIGHT
PROGRAM DIRECTIVE